

REMARKS

This Amendment is in response to an Office Action mailed November 26, 2007. In the Office Action, claim 12 has been objected to and claims 1-7, 9-16, 18-27, 29-44 and 46-47 are rejected under 35 U.S.C. §103(a). Reconsideration and withdrawal of the rejections in light of the Amendments and Remarks made herein is respectfully requested.

Request for Examiner's Interview

Applicants respectfully request the Examiner to contact the undersigned attorney by telephone at the phone number listed below if, after review, such claims are still not in condition for allowance. This telephone conference would greatly facilitate the examination of the subject application.

Claim Objection

Claim 12 has been objected based on an alleged informality. In response, Applicants have added a phrase requested by the Examiner. Withdrawal of the objection is respectfully requested.

Rejection Under 35 U.S.C. §103

Claims 1-9 and 11-15, 17-25 and 30-47 were rejected under 35 U.S.C. §103(a) as being unpatentable over England (U.S. Patent No. 6,938,164) in view of Schneier (Applied Cryptography) and Fries (U.S. Patent No. 7,036,023). Applicants respectfully traverse the rejection because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988).* Herein, the combined teachings of the cited references fail to describe or suggest all of the claim limitations.

For instance, with respect to independent claims 1, 12, 21, 32 and 39, Applicants respectfully submit that none of the cited references, either individually or in combination, describe or suggest a hash signing engine having a secure channel that signs (or the operation of signing) a computed cryptographic hash, the *signed* cryptographic hash being stored in a register in the memory of the computer that *is accessible by an outside entity to verify whether the content can be trusted. Emphasis added.* This “outside entity” is a device or user that is separate from the trustable operating system, computer or article of manufacturer implemented with the claimed invention. Herein, neither England, Schneier nor Fries, alone or in combination, describes or suggest accessibility of the signed cryptographic hash by an outside entity as claimed.

Furthermore, none of the cited references suggest loading content into the identified region (i.e., memory location of the trusted core) under control by the first processor. Rather, as set forth on page 3 of the Office Action, England teaches the CPU loading and executing instructions starting with the reset vector, but it appears that those components forming the trusted core are loaded into memory (110) from ROM 120 or storage devices (118) without being under control by the first processor. *See col. 5, lines 5-20 of England*. Thus, the first processor would not have any involvement in the loading of content in the identified region in order to load a trustable operating system.

Conclusion

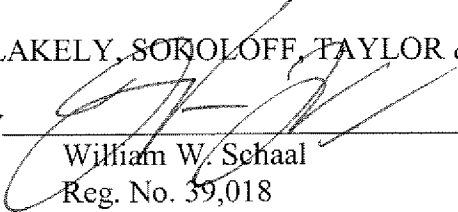
Applicants reserve all rights with respect to the applicability of the doctrine of equivalents. Applicants respectfully request that a timely Notice of Allowance be issued in this case and requests a telephone conference to discuss the allowability of the pending claims before issuance of any Office Action in order to facilitate prosecution of the subject application.

Respectfully submitted,

BLAKELY, SOLOLOFF, TAYLOR & ZAFMAN LLP

Dated: February 26, 2008

By


William W. Schaal

Reg. No. 39,018

Tel.: (714) 557-3800 (Pacific Coast)